REMARKS

Claim 11 has been amended to address an informality. No new subject matter has been added by way of this amendment. Claims 1-24 are pending in the application.

§103 Rejections

The Examiner rejected claims 1, 2, 4, 7, 8, 10, 11, 13, 20, 21 under 35 U.S.C. §103(a) as unpatentable over ***Zhang*** (US Patent Application No. 2005/0154895) in view of ***Paila*** (US Patent Application No. 2003/0096614). Applicants respectfully traverse this rejection for reasons more fully disclosed below.

Claim 1, which is directed to a method, calls, in part, for determining a private key for a first network based on at least one security value associated with a second network. The Examiner argues that the "session key" disclosed in ***Zhang*** corresponds to "private key" of claim 1, and the "3G network" corresponds to the "second network." The "session key" in ***Zhang***, however, is not determined based on a security value associated with the 3G network ("second network," according to the Examiner). Rather, ***Zhang*** describes that the "session key" is created by the WLAN server (not the 3G network), where the WLAN server then transmits the key to the user device to establish a communications session. *See* ***Zhang***, ¶24 (describing that WLAN creates a session key and encrypts the session key using the public key of the user device before transmitting it to the user device). Thus, contrary to the Examiner's suggestion, the "session key" in ***Zhang*** is not based on a "security value" associated with the 3G network.

Zhang does describe that the 3G network and the WLAN network have a pre-existing trust relationship. *See* ***Zhang***, ¶25. However, Zhang makes clear in ¶24 that the "session key" (which the Examiner calls the "private key") is determined by the WLAN server using the user device's public key, and is not determined based on any "security value" associated with the 3G network.

Additionally, the "session key" in ***Zhang*** is not a "private key" of claim 1. As is well-established, the claims must be construed in view of the specification. Here the specification provides that the term "private key" refers to a key, that once calculated, is not shared with another device. *See* Patent Application, p.18, lines 10-12. The Examiner, unfortunately, simply ignores the specification, and reads the claims in a vacuum. This is clearly improper. Unlike the "private key" of claim 1, the "session key" of ***Zhang*** describes that the "session key" is created by the WLAN server and then transmitted to the user device to establish a session. *See* ***Zhang***, ¶24. Because the "session key" in ***Zhang*** is shared with another device after it is determined (in this case with the user device), the "session key" is not a "private key" as that term is used in the claims and the specification.

In view of at least the aforementioned reasons, claim 1 and its dependent claims are allowable. Additionally, the other independent claims and their respective dependent claims are also allowable for the same reasons.

In regard to certain of the dependent claims, the Office Action is traversed for at least the further reasons presented below. Claim 2 calls for determining the private key based on a shared secret data key associated with the cellular network. With respect to this feature, the Examiner argues that ***Zhang*** discloses in paragraph 24 determining a session key based on a shared secret data key associated with the 3G network ("cellular network," according to the Examiner). The Applicants respectfully disagree. Paragraph 24 of ***Zhang*** describes that it is the WLAN server 230 that determines the session key ("private key," according to the Examiner). Notably, ***Zhang*** further describes that the session key that is generated by the WLAN server 230 is then transmitted to a user device through the 3G network. *See* ***Zhang***, ¶24. Thus, notwithstanding the Examiner's assertion to the contrary, ***Zhang*** simply does not disclose or suggest determining the session key based on any shared secret data key associated with the 3G network. For at least

this reason, the Applicants submit that claim 2 is allowable. For substantially the same reasons, it is submitted that claim 12 is also allowable.

Claim 4 calls for populating the private key with a cryptographic transform of the shared secret data key. The Examiner alleges this feature is taught in paragraph 24 of ***Zhang***. The cited paragraph describes encrypting a session key using a public key of the user device. It does not, however, describe a cryptographic transform, and certainly does not describe populating the private key with such a transform of the shared secret data key, as called for by claim 4. For at least this reason, it is submitted that claim 4 is allowable. For substantially the same reasons, it is submitted that claim 13 is allowable.

For the aforementioned reasons, it is respectfully submitted that all claims pending in the present application are in condition for allowance. The Examiner is invited to contact the undersigned at (713) 934-4064 with any questions, comments or suggestions relating to the referenced patent application and this response.

Respectfully submitted,

Date: October 2, 2007

/Ruben S. Bains/

Ruben S. Bains
Reg. No. 46,532
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-4064
(713) 934-7011 (Fax)
AGENT FOR APPLICANTS